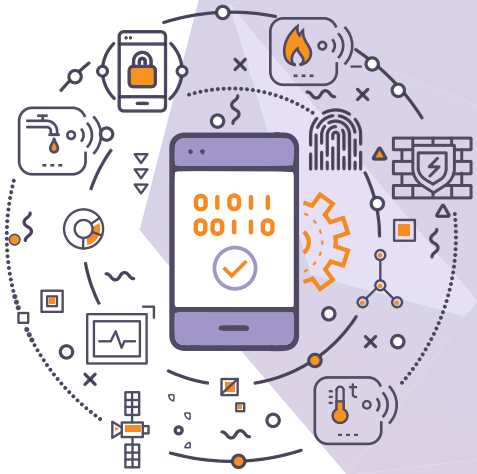


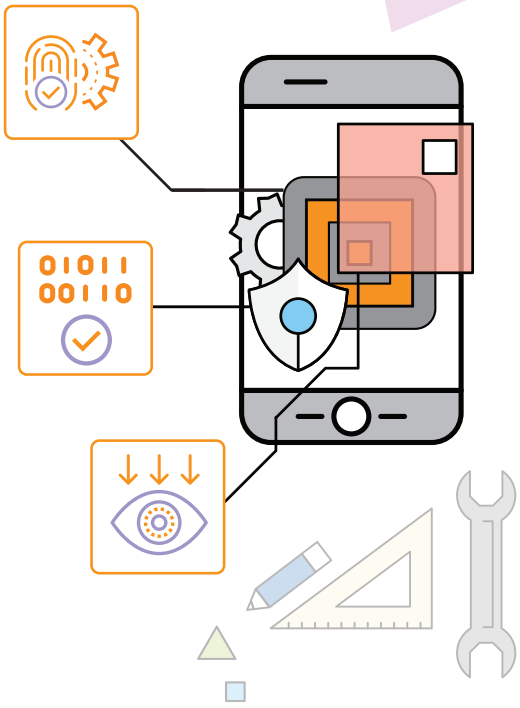
Positronic

Trusted Device

HIGH ASSURANCE DEVICE IDENTIFICATION, STORAGE, AND HARDWARE TRUSTED UI USING TEE TECHNOLOGY

Positronic Trusted Apps run inside the device Trusted Execution Environment (TEE) hardware to establish trust in dealing with the same device and hardware control over the device UI peripherals independent of the device Operating System.

Positronic Capabilities



Positronic-ID trusted app for high assurance device identification using hardware-based liveness validation of device identity . Existing mobile apps can use the Positronic-ID to gain access to the internal APIs of organisation. Positronic-ID can be used with an API Gateway to submit the authentication credentials of the device rather than the user login credentials

Positronic trusted apps run inside the device TEE hardware to establish trust in dealing with the same device independent of the device rich operating system, providing anti-cloning protection, malware and device root access resilience, hardware-level cryptography and key protection

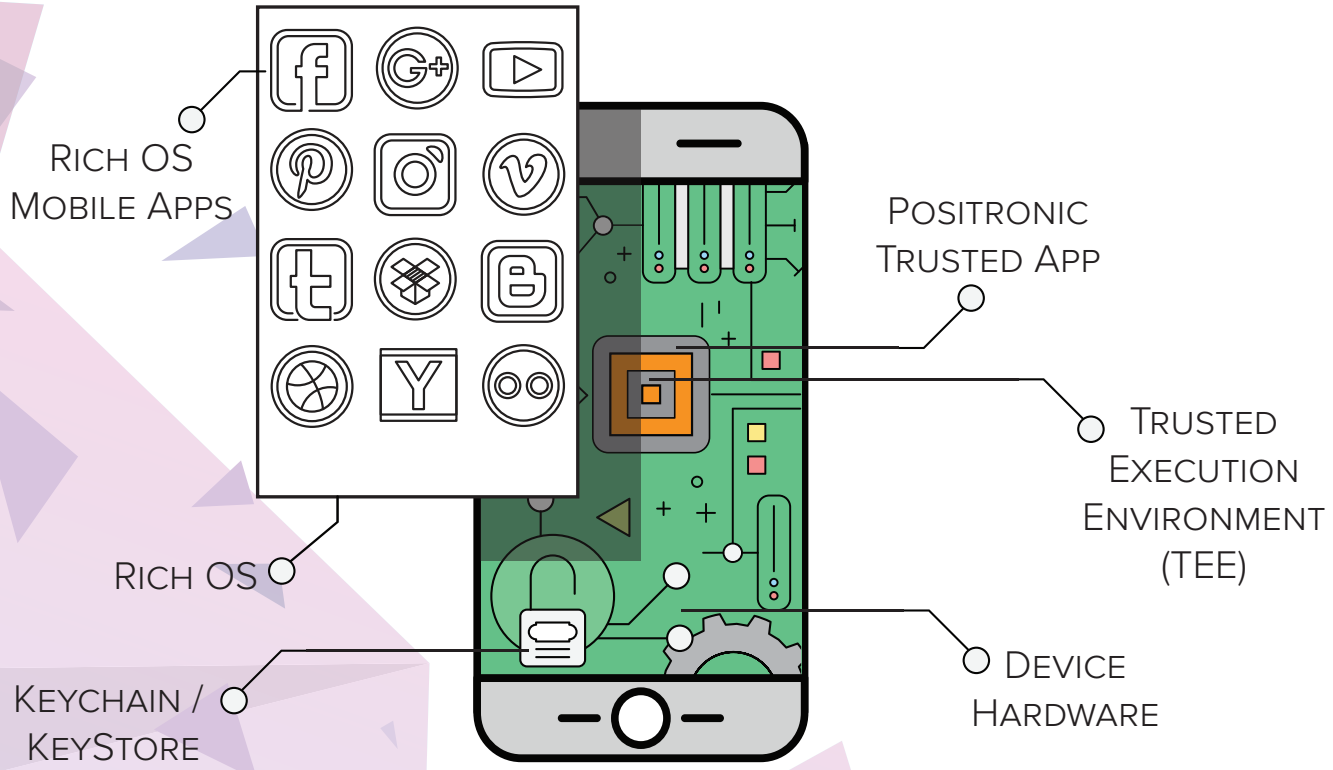
Positronic-Signer trusted app with hardware controlled Trusted-UI that uses TEE technology to perform Salt mSign style authentication end-to-end from Echidna to Positronic; and Payment Card PIN entry into TEE hardware controlled Trusted-UI

TEE Technology

Trusted Execution Environment (TEE) resides within the main processor of mobile phones and IoT devices. Positronic Trusted Apps run within the TEE in a secure operating system that runs alongside the normal rich operating system (e.g. Android).

TEE technology is embedded into devices during chip manufacturing. Positronic Trusted Apps are post-deployed into the TEE. Positronic Trusted Apps use the TEE to ensure that sensitive data is stored, processed and protected in a trusted and physically isolated environment.

Positronic Trusted Apps use TEE technology to drive secure peripherals such as Trusted User Interface where the display and touchpad is secured independent of the rich operating system, delivering the ability to perform functions such as Payment Card PIN entry and Salt mSign style authentication with TEE hardware secured WYSIWYS (What You See Is What You Sign).



- Positronic Trusted Apps are secured by hardware
- Security based on hardware Roots of Trust
- Secure code execution and storage
- Secured interaction between the user and the Positronic Trusted App
- TEE technology is proven and embedded into over one billion devices
- Supported on Samsung ARTIK Smart IoT .

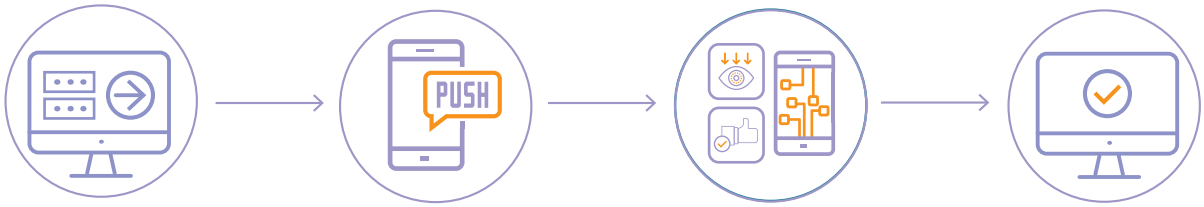
‘Silent’ Device Authentication

User Launches Mobile Banking App Without Sign-In Requests to Retrieve Wealth Portfolio Information & Balances

Positronic Trusted App Generates a High Assurance and Anti-Cloneable Device Fingerprint to Authenticate the User’s Registered Device

User Receives and Views Wealth Portfolio Information & Balances on the Mobile Banking App Without needing to Sign-In to the App

Trusted UI for Authentication



User Initiates an Internet Banking Transaction where the Risk Engine requires Additional Authentication

User Receives a Push Notification on their Registered Mobile App with Positronic-Signer Embedded Token

Transaction Summary is Decrypted and Displayed by Positronic-Signer in TEE Hardware Controlled Trusted UI. The User ‘Approves’ the Summary

Internet Banking Transaction Authentication is Completed

Salt Group Pty Ltd
Level 30, 459 Collins Street
Melbourne VIC 3000
Australia

Australia & Asia Pacific
T: +61-3-9614-4416
F: +61-3-9614-2992
E: sales@saltgroup.com.au